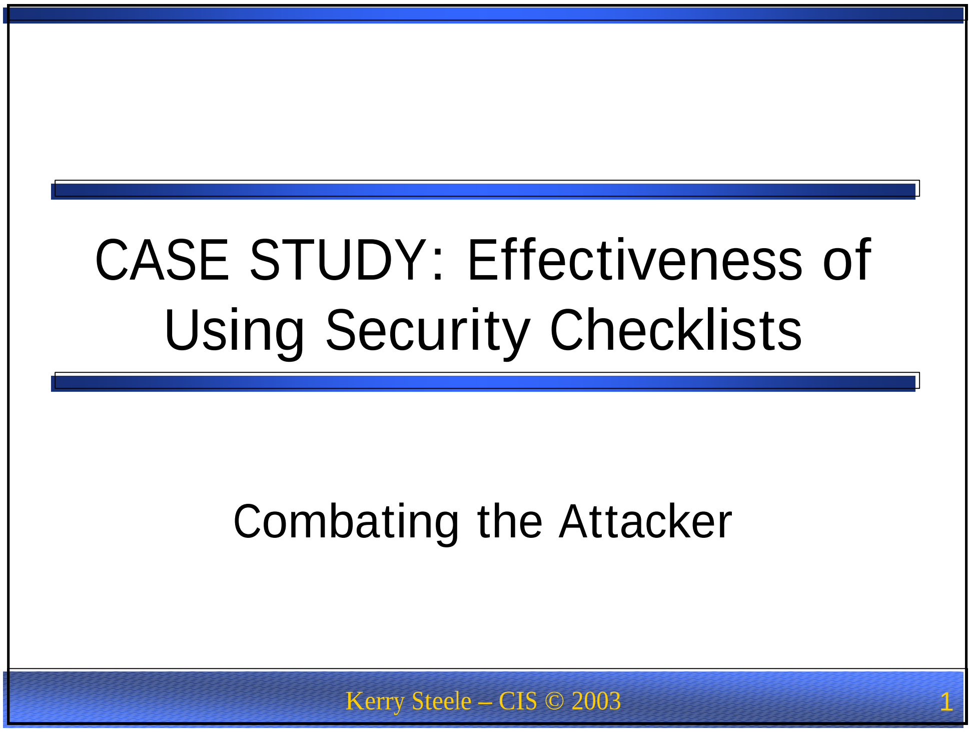
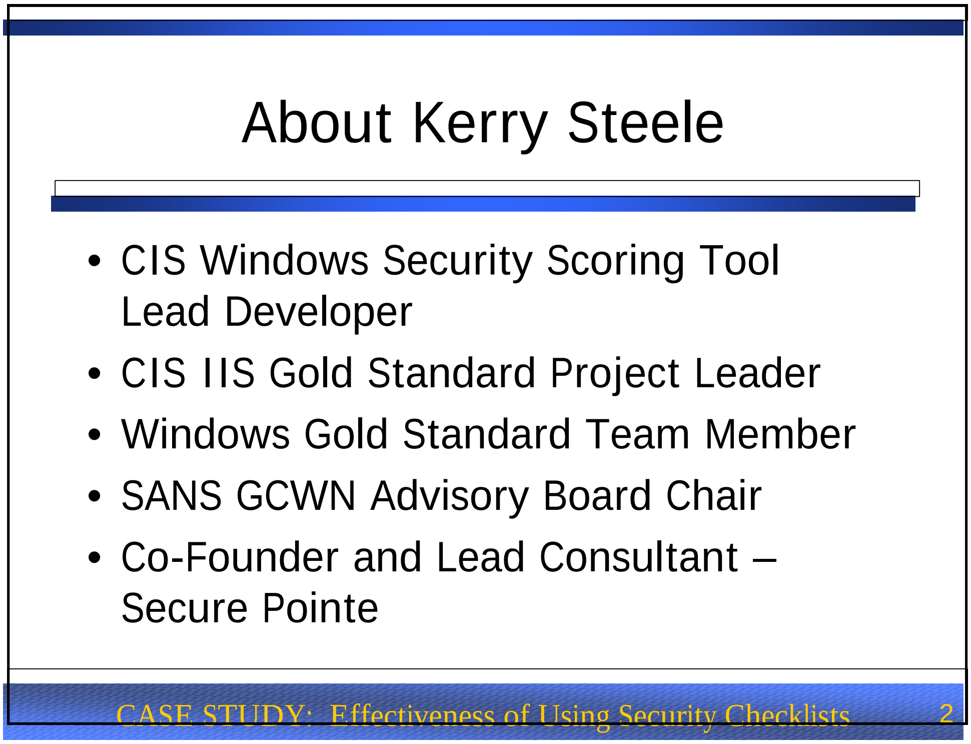


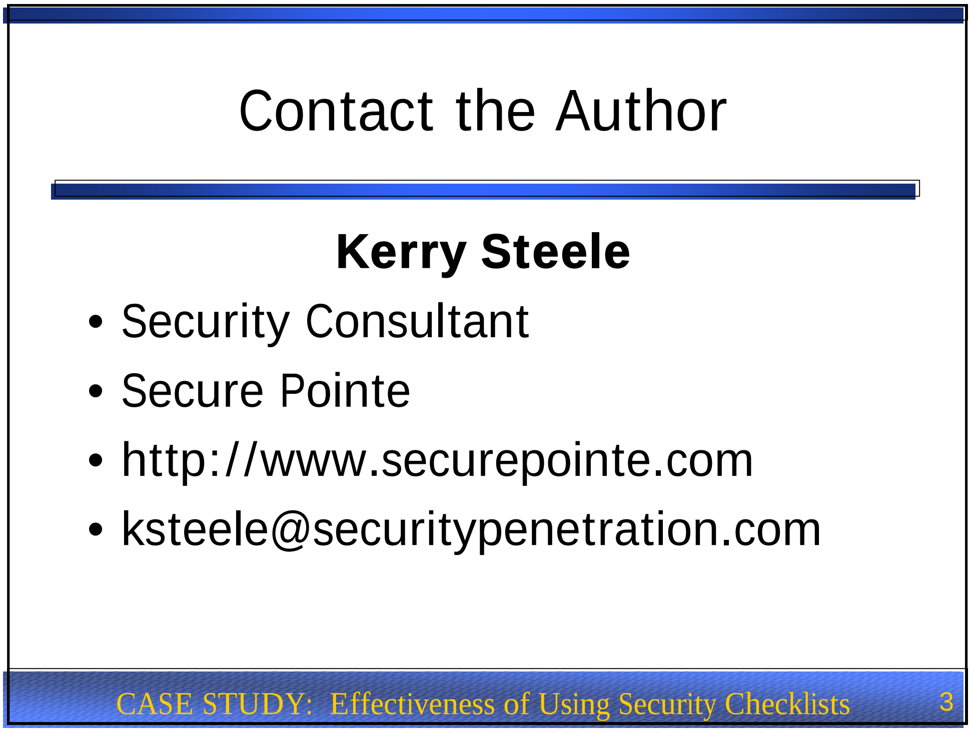
CASE STUDY: Effectiveness of Using Security Checklists

Combating the Attacker



About Kerry Steele

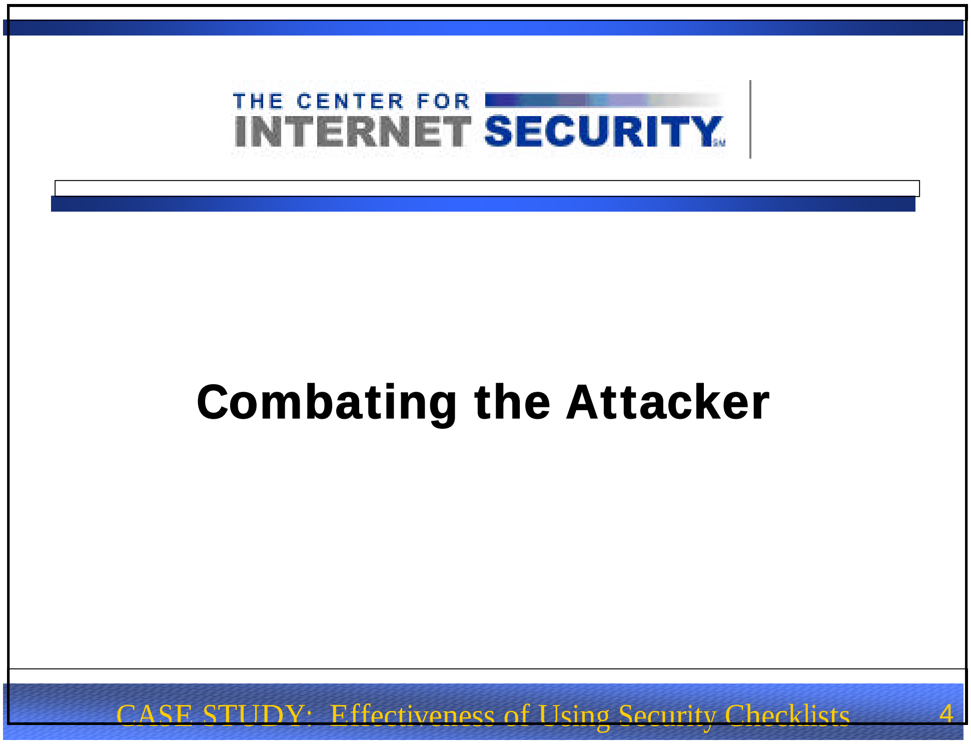
- CIS Windows Security Scoring Tool Lead Developer
- CIS IIS Gold Standard Project Leader
- Windows Gold Standard Team Member
- SANS GCWN Advisory Board Chair
- Co-Founder and Lead Consultant – Secure Pointe



Contact the Author

Kerry Steele

- Security Consultant
- Secure Pointe
- http://www.securepointe.com
- ksteele@securitypenetration.com



THE CENTER FOR INTERNET SECURITY

Combating the Attacker

THE CENTER FOR INTERNET SECURITY

CASE STUDY:

Vulnerability Assessment of Machines Configured with the Gold Standard Security Benchmark

We have met the enemy, and it is us

“Through 2005, 90 percent of cyber attacks will continue to exploit known security flaws for which a patch is available or a preventive measure known.”

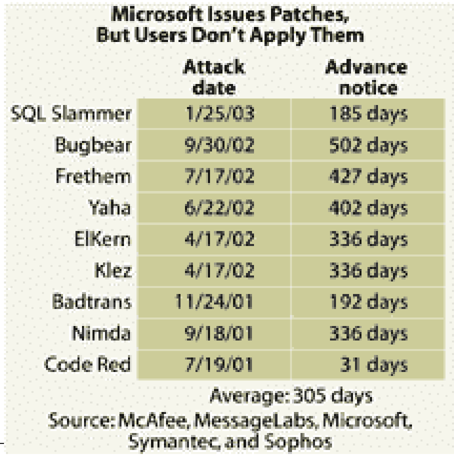
» Gartner Group, May 6, 2002

We have met the enemy, and it is us

> *"Many recent cyber attacks could have been avoided if enterprises were more focused on their security efforts, but users seem not to learn from their mistakes."*

» Gartner Group, May 6, 2002

Microsoft Issues Patches, But Users Don't Apply Them



Microsoft Issues Patches, But Users Don't Apply Them

	Attack date	Advance notice
SQL Slammer	1/25/03	185 days
Bugbear	9/30/02	502 days
Frethem	7/17/02	427 days
Yaha	6/22/02	402 days
ElKern	4/17/02	336 days
Klez	4/17/02	336 days
Badtrans	11/24/01	192 days
Nimda	9/18/01	336 days
Code Red	7/19/01	31 days

Average: 305 days

Source: McAfee, MessageLabs, Microsoft, Symantec, and Sophos

Forrester Research
April 3, 2003

Patch Maintenance – Service Packs and Hotfixes

- It Is Almost Impossible to Keep Up With Microsoft Patches!
- Ongoing maintenance is a pain
  - Apply the latest service packs, security rollup packages, cumulative patches, and all necessary security hotfixes as identified by the CIS hotfix checking technology employed.
- Develop a process:
  - Ensure Hotfixes are current
    - Manually (Custom scripting solutions or Sneaker-net)
    - Commercial Tools (SUS, SMS, HFNetChk Pro, UpdateExpert, Hercules, etc.)
  - Get current security information
    - http://www.microsoft.com/technet/security/bulletin/notify.asp
    - Other mailing lists – SecurityFocus

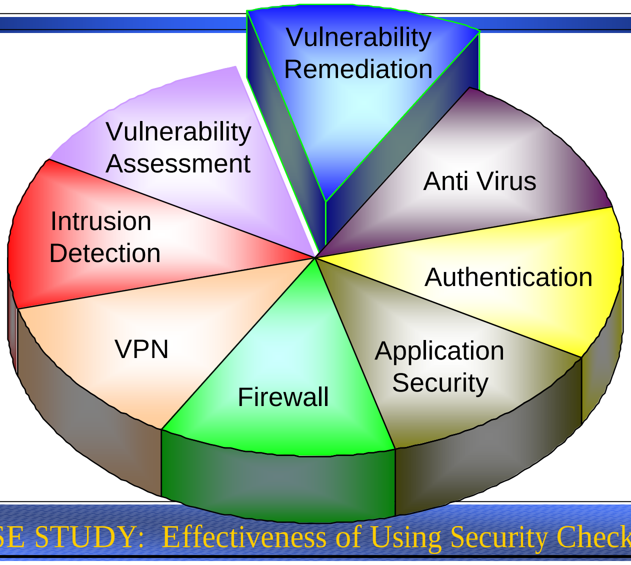
5 Classes of Vulnerabilities

1. Insecure Accounts
   - Null Password, Admin no PW, no PW expiration...
2. Unnecessary Services
   - Telnet, Remote Access, Remote Exe...
3. Backdoors
   - NETBUS, BACKORIFICE, SUBSEVEN...
4. Mis-configurations
   - NetBIOS null sessions...
5. Software Defects
   - Hot-fixes, Patches...

The top 4 classes are device access methods.

Patches do not address device access methods.

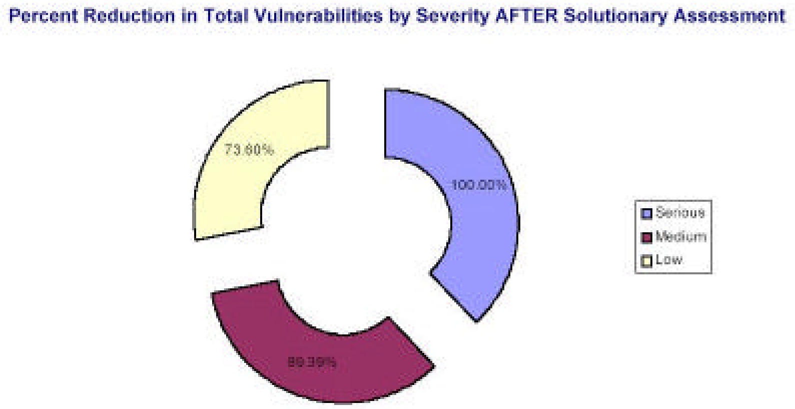
Remediation Completes the Security Circle



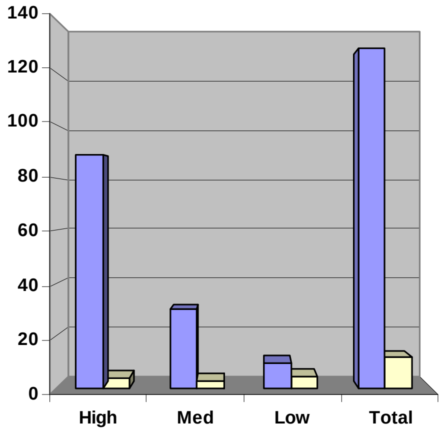
The Good News

- The consensus security benchmark settings developed by the CIS teams eliminates 80-90% of the vulnerabilities that are being exploited by cyber-attackers
- There is an abundance of low-hanging fruit we all can pick to substantially reduce our risk of unauthorized intrusion.

Case Study Available at www.cisecurity.org



NSA Case Study



	High	Med	Low	Total
□ W2K Default Load	89	30	10	129
□ W2K w/Config. Guide & Patches	4	3	5	12

% Reduction: 96 90 50 91

Yet another study (Mitre):

- Windows 2000 Professional Gold Standard configuration reduced CVE vulnerabilities by 83%

IA Newsletter describing the NSA and Mitre studies

- Vol 5, Number 3, Fall 2002
- http://iac.dtic.mil/iatac/news_events/ia_newsletter.htm

CIS Standards Mitigate Vulnerabilities

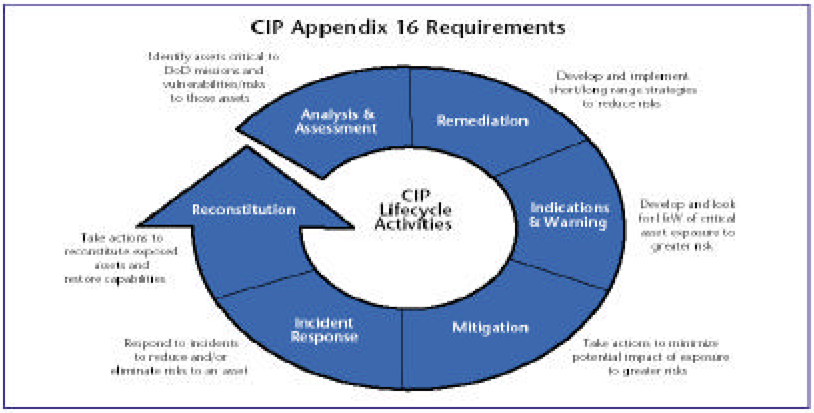

CIP Appendix 16 Requirements
Identify assets critical to DoD missions and vulnerabilities/risks to those assets
Analysis & Assessment
Remediation
Develop and implement short/long range strategies to reduce risks
CIP Lifecycle Activities
Reconstitution
Indications & Warning
Develop and look for I&W of critical asset exposure to greater risk
Take actions to reconstitute exposed assets and restore capabilities
Incident Response
Mitigation
Respond to incidents to reduce and/or eliminate risks to an asset
Take actions to minimize potential impact of exposure to greater risks

Figure 1. DoD CIP lifecycle activities

THE CENTER FOR INTERNET SECURITY

Case Studies:

Vulnerability Assessment of Machines Configured with the Gold Standard Security Benchmark:

LIVE DATA

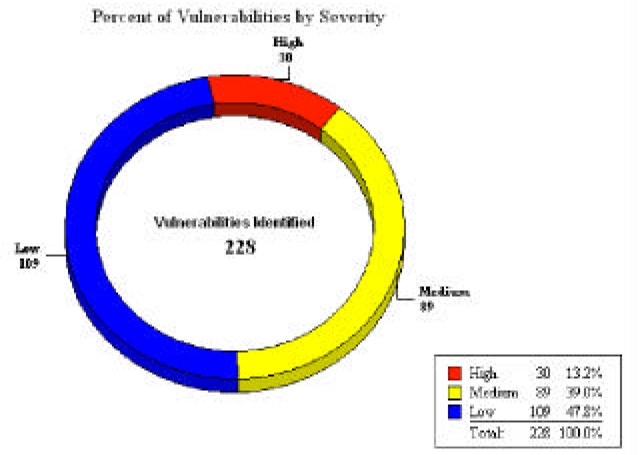
Selecting a Vulnerability Assessment (VA) Tool

- Caveat Emptor
- Use more than one tool. WHY?
  - False Positives
  - False Negatives
- Host-based or Network-based – each has it's trade-offs – IT DEPENDS
- CIS Tools are Host-based VA tools
- http://www.infosecuritymag.com/2003/mar/cover.shtml

Research methodology

1. Scan a system "out of the box" and list identified vulnerabilities
2. Configure the system with the appropriate benchmark
3. Rescan the system and note the vulnerabilities remaining

Vulnerability Assessment of Windows 2000 Server (Default)

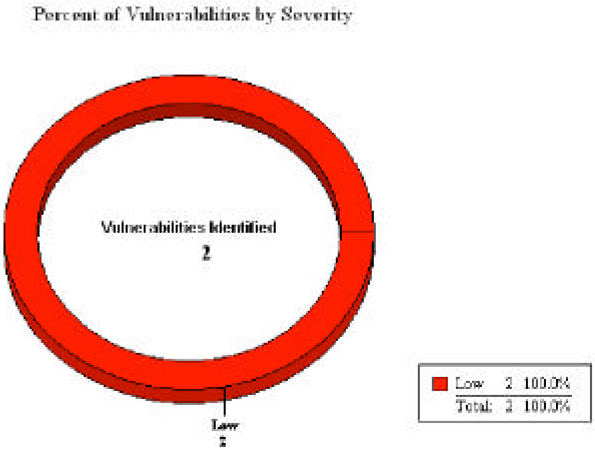


Vulnerability Assessment of Windows 2000 Server (Default)

ISS Internet Scanner 6.2.1

• High:	30
• Medium:	89
• Low:	109
• Total:	228

Vulnerability Assessment of Windows 2000 Server (Post CIS)



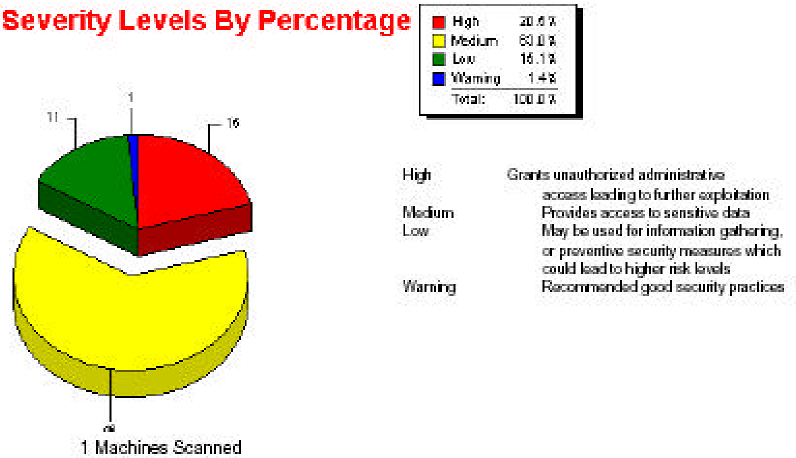
Vulnerability Assessment of Windows 2000 Server (Post CIS)

ISS Internet Scanner 6.2.1

High:	0	100%
Medium:	0	100%
Low:	2 (ping and tracert)	98%
Total:	2 (acceptable risk)	99%

- Resulting in a 99% (100%) reduction of network vulnerabilities for this device.

Vulnerability Assessment of RedHat 7.1 (Default)



High Grants unauthorized administrative access leading to further exploitation
Medium Provides access to sensitive data
Low May be used for information gathering, or preventive security measures which could lead to higher risk levels
Warning Recommended good security practices

Vulnerability Assessment of RedHat 7.1 (Default)

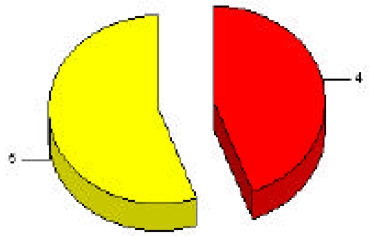
Harris STAT Scanner 5.11

- High: 15
- Medium: 46
- Low: 11
- Warning: 1
- Total: 73

Vulnerability Assessment of RedHat 7.1 (Post CIS)

Severity Levels By Percentage

🟥	High	44.4%
🟨	Medium	55.6%
	Total:	100.0%



High	Grants unauthorized administrative access leading to further exploitation
Medium	Provides access to sensitive data
Low	May be used for information gathering, or preventive security measures which could lead to higher risk levels
Warning	Recommended good security practices

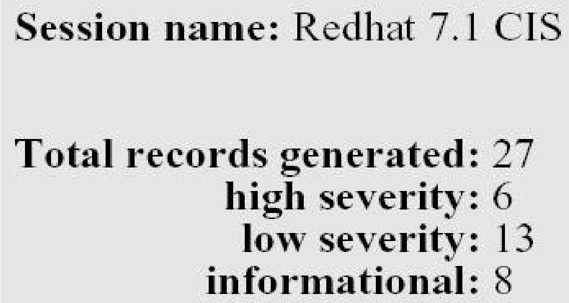
1 Machines Scanned

Vulnerability Assessment of RedHat 7.1 (Post CIS)

Harris STAT Scanner 5.11

- High: 4 (all false positive) 73%
- Medium: 5 (all false positive) 89%
- Low: 0 100%
- Warning: 0 100%
- Total: 9 (effectively zero) 88%
- Resulting in a 88% reduction in vulnerabilities for this device (100%)

Vulnerability Assessment of RedHat 7.1 (Default)



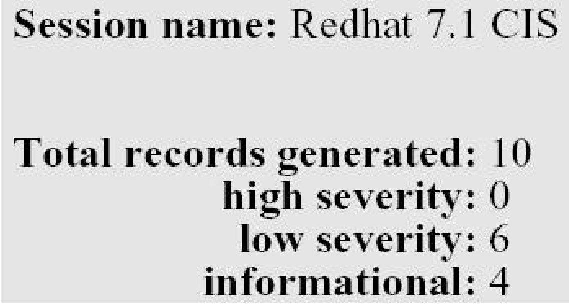
Session name: Redhat 7.1 CIS

Total records generated: 27
high severity: 6
low severity: 13
informational: 8

Vulnerability Assessment of RedHat 7.1 (Default)

	Nessus
• High:	6
• Low:	13
• Informational:	8
• Total:	27

Vulnerability Assessment of RedHat 7.1 (Post CIS)



Session name: Redhat 7.1 CIS

Total records generated: 10
high severity: 0
low severity: 6
informational: 4

Vulnerability Assessment of RedHat 7.1 (Post CIS)

	Nessus	
• High:	0	100%
• Low:	6 (2 false +)	54%
• Informational:	4	50%
• Total:	10	63%

- 63% reduction in vulnerabilities for this device (70% or 100%)

Conclusions

- Use of the consensus security benchmarks results in a very substantial reduction in the risk of unauthorized intrusion.
- Gold Standard and similar security checklists reduce 80-90% of a devices vulnerabilities and exposure on the network.
- Security staffs are thereby able to focus their time on the more manageable number of remaining threats to the information residing on their systems.
- Consensus projects and collaboration are the keys to success.

Contact the Author

Kerry Steele

- Security Consultant
- Secure Pointe
- http://www.securepointe.com
- ksteele@securitypenetration.com

THE CENTER FOR INTERNET SECURITY

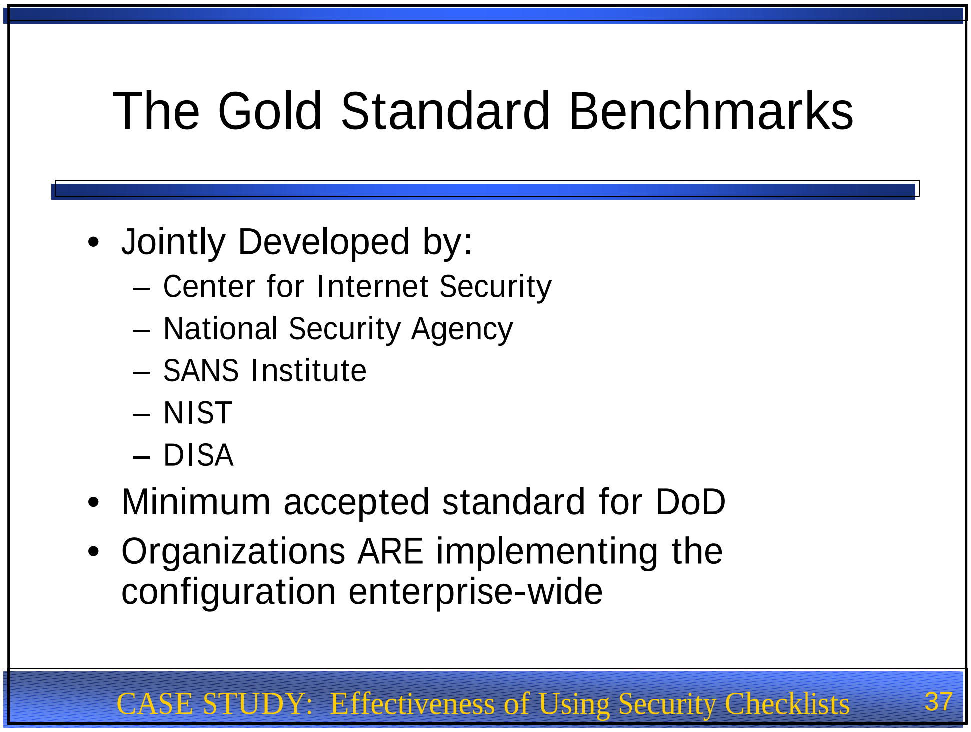
Appendix:

What's going on at CIS in the Windows world?

CIS Benchmark and Scoring Tool Development

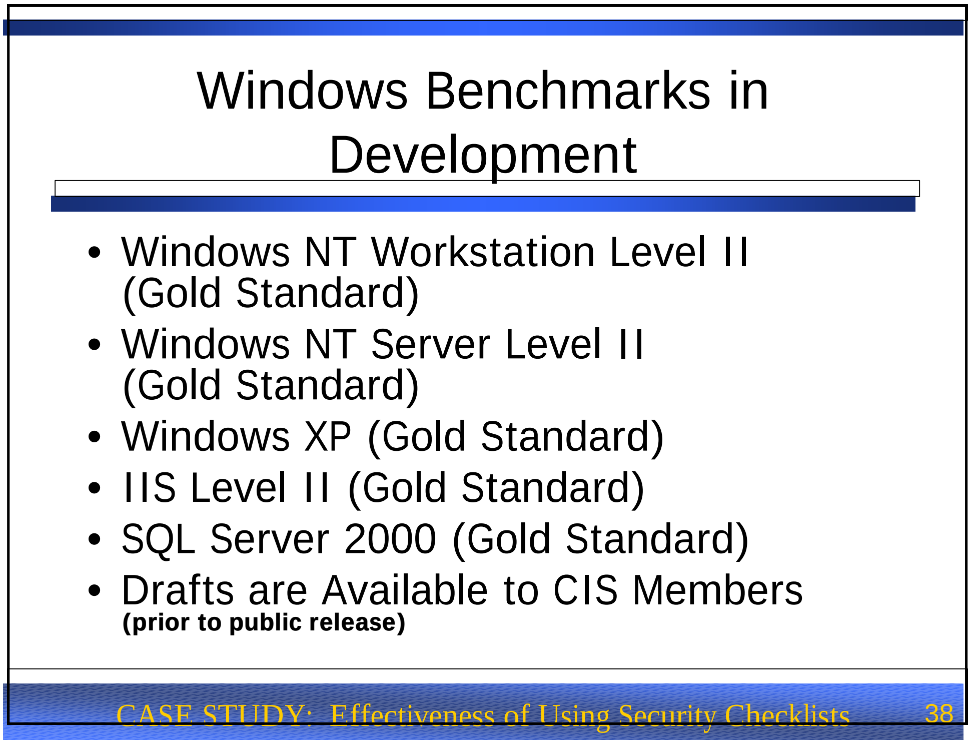
Windows Benchmarks – Currently Available to the Public

- Windows 2000 Professional Level II (Gold Standard)
- Windows 2000 Server Level II (Gold Standard)
- Windows 2000 Level I (Both Server & Workstation)
- Windows NT Level I (Both Server & Workstation)



The Gold Standard Benchmarks

- Jointly Developed by:
  - Center for Internet Security
  - National Security Agency
  - SANS Institute
  - NIST
  - DISA
- Minimum accepted standard for DoD
- Organizations ARE implementing the configuration enterprise-wide



Windows Benchmarks in Development

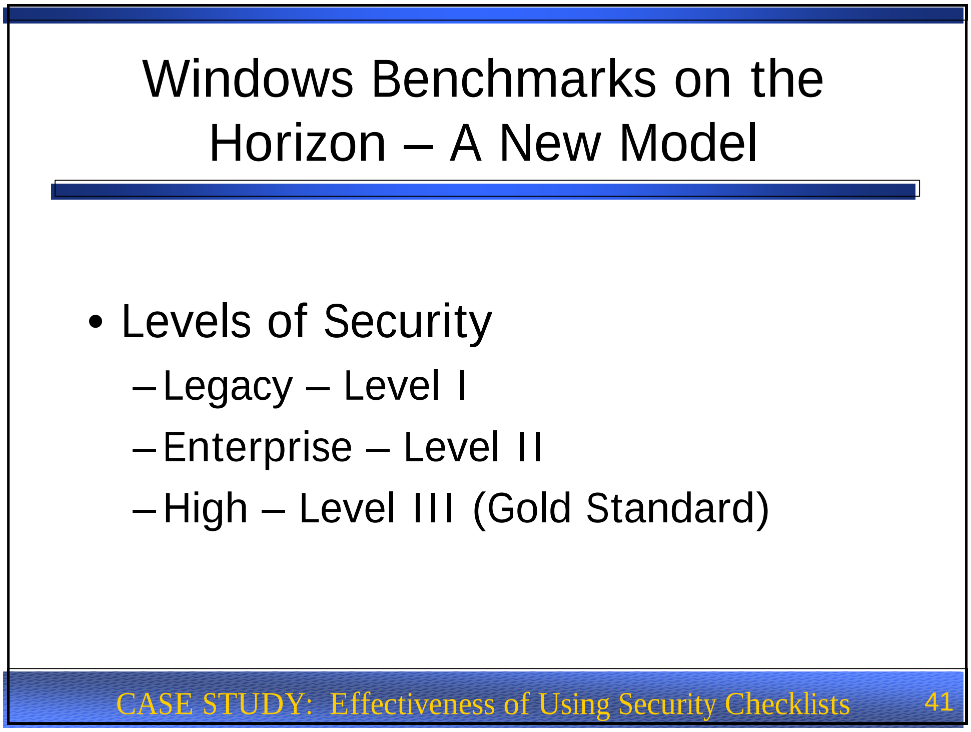
- Windows NT Workstation Level II (Gold Standard)
- Windows NT Server Level II (Gold Standard)
- Windows XP (Gold Standard)
- IIS Level II (Gold Standard)
- SQL Server 2000 (Gold Standard)
- Drafts are Available to CIS Members **(prior to public release)**

Windows Benchmarks on the Horizon

- Windows Server 2003
- Exchange Server 2000
- You tell us – this is driven by the CIS Membership

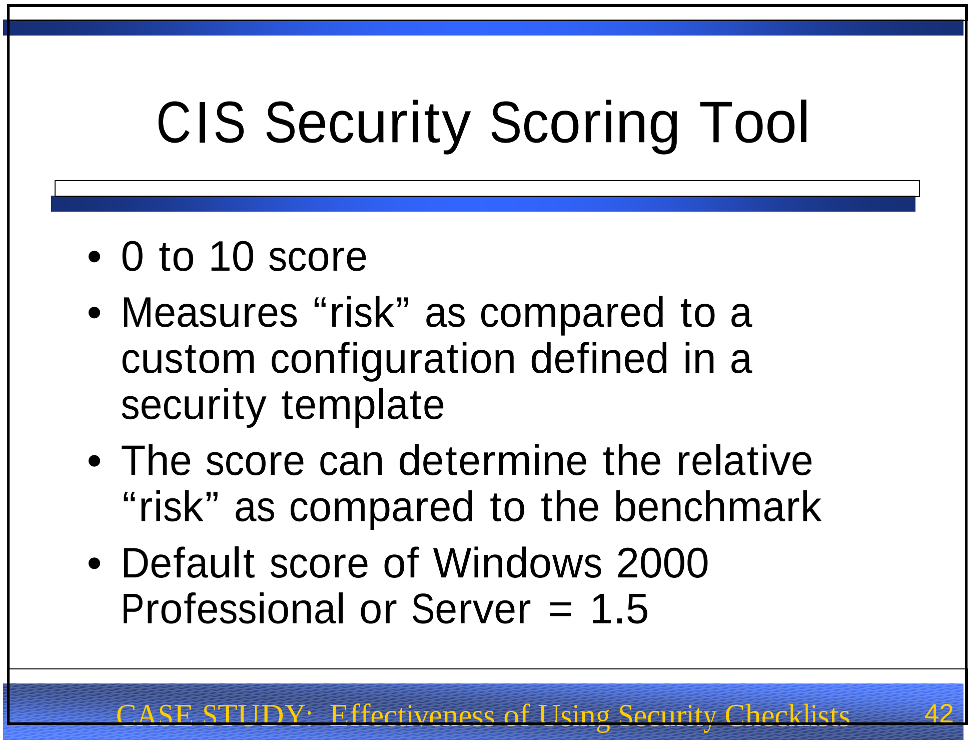
Windows Benchmarks on the Horizon – A New Model

- Role-based security benchmarks
  - Domain member workstation
  - Domain member server
  - Domain Controller
  - Standalone workstation
  - Standalone server
  - Laptop
  - Bastion Server



Windows Benchmarks on the Horizon – A New Model

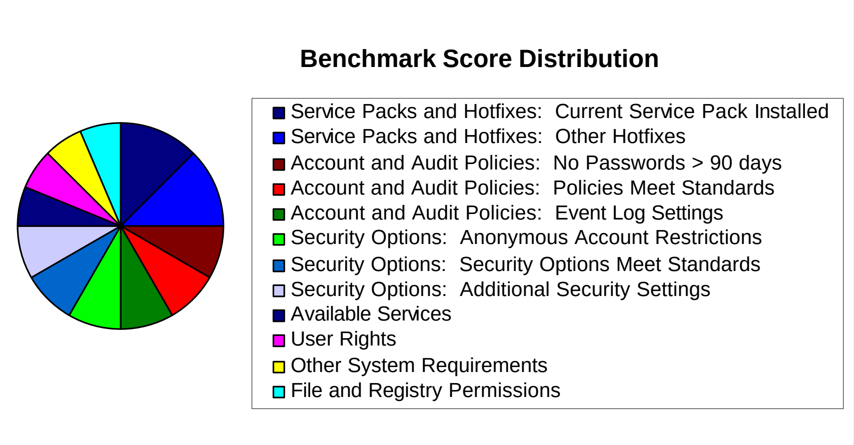
- Levels of Security
  - Legacy – Level I
  - Enterprise – Level II
  - High – Level III (Gold Standard)



CIS Security Scoring Tool

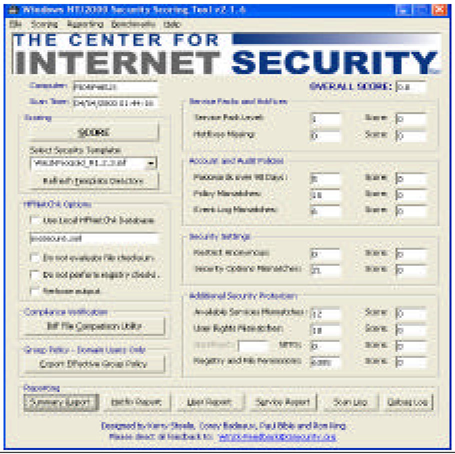
- 0 to 10 score
- Measures “risk” as compared to a custom configuration defined in a security template
- The score can determine the relative “risk” as compared to the benchmark
- Default score of Windows 2000 Professional or Server = 1.5

Score Categories and Weights



CIS Security Scoring Tool

- Non-invasive, Host-based security scanning tool gives a SCORE
- Internally uses SeCEdit and HFNetChk
- Score / Compliance
- Audit local configuration using ANY security template
- 10 may not be usable
- There is NO silver bullet


Windows NT/2000 Security Scoring Tool v2.1.4
File Scoring Reporting Benchmarks Help
THE CENTER FOR INTERNET SECURITY
Computer:
Scan Time:
OVERALL SCORE:
Scoring
SCORE
Select Security Template
Refresh Template Directory
HFNetChk Options
Use Local HFNetChk Database
Compliance Verification
Inf File Comparison Utility
Group Policy - Domain Users Only
Export Effective Group Policy
Service Packs and Hotfixes
Service Pack Level:
Hotfixes Missing:
Account and Audit Policies
Policy Mismatches:
Event Log Mismatches:
Security Settings
Security Options Mismatches:
Additional Security Protection
Available Services Mismatches:
User Rights Mismatches:
Registry and File Permissions:
Score:
Reporting
Summary Report
Service Report
Scan Log

How is scoring done?

- Host-based – local scan only
- Use SeCEdit to compare configuration against custom security templates distributed with the tool
- Run Microsoft/Shavlik’s HFNetChk Network Security Hotfix Checker
- Windows API calls

Tool Enhancements: Coming soon

- Advanced Security Hotfix Checking Technology
- CIS Command-line Scoring Tool
- Advanced Detailed Reporting in XML
- Enterprise Report collection
- Score History (track scores over time)
- Customization: (report destination including network location, exclude specified accounts, category weights)

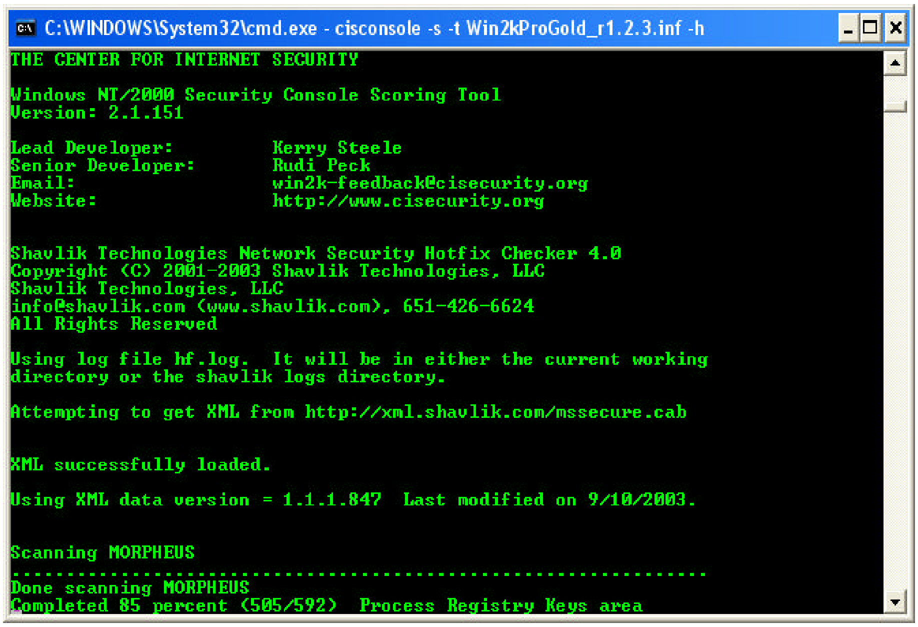
Tool Enhancements: On the Horizon

- What else...?
- See the readme.txt distributed with the CIS Security Scoring Tool for the long list

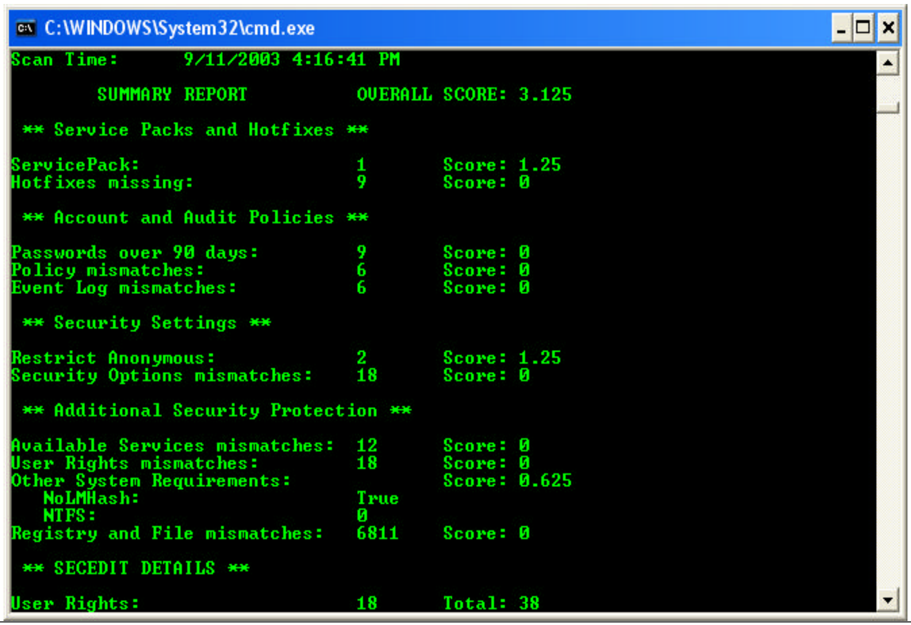
THE CENTER FOR INTERNET SECURITY

CIS Security Scoring Tool Preview:

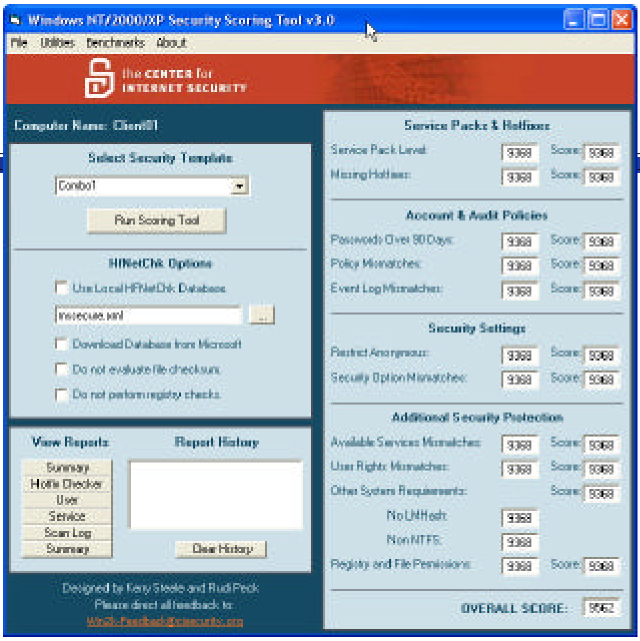
3.0 GUI and Command-line Versions


C:\WINDOWS\System32\cmd.exe - cisconsole -s -t Win2kProGold_r1.2.3.inf -h

```
THE CENTER FOR INTERNET SECURITY

Windows NT/2000 Security Console Scoring Tool
Version: 2.1.151

Lead Developer:         Kerry Steele
Senior Developer:       Rudi Peck
Email:                  win2k-feedback@cisecurity.org
Website:                http://www.cisecurity.org


Shavlik Technologies Network Security Hotfix Checker 4.0
Copyright (C) 2001-2003 Shavlik Technologies, LLC
Shavlik Technologies, LLC
info@shavlik.com (www.shavlik.com), 651-426-6624
All Rights Reserved

Using log file hf.log.  It will be in either the current working
directory or the shavlik logs directory.

Attempting to get XML from http://xml.shavlik.com/mssecure.cab


XML successfully loaded.

Using XML data version = 1.1.1.847  Last modified on 9/10/2003.


Scanning MORPHEUS
................................................................
Done scanning MORPHEUS
Completed 85 percent (505/592)  Process Registry Keys area
```



```
Scan Time:       9/11/2003 4:16:41 PM

        SUMMARY REPORT          OVERALL SCORE: 3.125

 ** Service Packs and Hotfixes **

ServicePack:                    1       Score: 1.25
Hotfixes missing:               9       Score: 0

 ** Account and Audit Policies **

Passwords over 90 days:         9       Score: 0
Policy mismatches:              6       Score: 0
Event Log mismatches:           6       Score: 0

 ** Security Settings **

Restrict Anonymous:             2       Score: 1.25
Security Options mismatches:    18      Score: 0

 ** Additional Security Protection **

Available Services mismatches:  12      Score: 0
User Rights mismatches:         18      Score: 0
Other System Requirements:              Score: 0.625
   NoLMHash:                    True
   NTFS:                        0
Registry and File mismatches:   6811    Score: 0

 ** SECEDIT DETAILS **

User Rights:                    18      Total: 38
```



Computer Name: Client01

Select Security Template

Combo1

HfNetChk Options

□ Use Local HFNetChk Database

insecure.xml

□ Download Database from Microsoft

□ Do not evaluate file checksums

□ Do not perform registry checks

View Reports

Report History

Designed by Kerry Steele and Rudi Peck
Please direct all feedback to:
Win2k-Feedback@cisecurity.org

Service Packs & Hotfixes

Service Pack Level: 9368 Score: 9368

Missing Hotfixes: 9368 Score: 9368

Account & Audit Policies

Passwords Over 90 Days: 9368 Score: 9368

Policy Mismatches: 9368 Score: 9368

Event Log Mismatches: 9368 Score: 9368

Security Settings

Restrict Anonymous: 9368 Score: 9368

Security Option Mismatches: 9368 Score: 9368

Additional Security Protection

Available Services Mismatches: 9368 Score: 9368

User Rights Mismatches: 9368 Score: 9368

Other System Requirements: Score: 9368

No LMHash: 9368

Non NTFS: 9368

Registry and File Permissions: 9368 Score: 9368

OVERALL SCORE: 9562

THE CENTER FOR INTERNET SECURITY

Contact List – Windows NT/2000/XP/2003

- Jeff Shawgo – Benchmark Editor Win2k-Bench@cisecurity.org
- Kerry Steele – Scoring Tool Developer Win2k-Scan@cisecurity.org
- General Feedback – **Win2K-Feedback@cisecurity.org**